UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA v. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, Defendants.	Case No. 24 Cr. 82 (RMB)

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT WILLIAM HILL'S MOTION TO SUPPRESS EVIDENCE OBTAINED THROUGH THE SEIZURE AND SEARCH OF HIS STORED ELECTRONIC COMMUNICATIONS

Roger A. Burlingame
Matthew L. Mazur
DECHERT LLP
Three Bryant Park
1095 Avenue of the Americas
New York, NY 10036
Tel.: +1 212 698 3500
roger.burlingame@dechert.com
matthew.mazur@dechert.com

Counsel for Defendant William Lonergan Hill

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

PRELIMINARY STATEMENT 1

BACKGROUND 3

LEGAL STANDARD 7

ARGUMENT 9

I. THE PEÑA AFFIDAVIT CONTAINED FALSE AND MISLEADING STATEMENTS THAT ARE MATERIAL TO PROBABLE CAUSE 9

II. THERE WAS NO PROBABLE CAUSE TO CONCLUDE THAT SAMOURAI WALLET WAS AN UNLICENSED MONEY TRANSMITTING BUSINESS OR THAT EVIDENCE OF MONEY LAUNDERING OR OTHER CRIMES BY ITS USERS WOULD BE FOUND IN MR. HILL'S PERSONAL GMAIL ACCOUNT 11

A. The Peña Affidavit Failed To Establish Probable Cause To Conclude That Samourai Wallet Was An Unlicensed Money Transmitting Business 11

B. The Peña Affidavit Failed To Establish Probable Cause That Evidence of Money Laundering or Sanctions Evasion Would Be Found in Mr. Hill's Personal Gmail Account 12

III. THE GMAIL SEARCH WARRANT WAS IMPERMISSIBLY OVERBROAD UNDER THE FOURTH AMENDMENT 13

A. Where the Underlying Probable Cause is Narrow, Search Warrants Authorizing the Wholesale Search and Seizure of a Person's Email Account are Impermissible Under the Fourth Amendment 13

B. The Warrant Did Not Provide Meaningful Guidance As To What Data Fell Within The Purview Of The Warrant 15

C. The Government Must Return or Destroy Any Data Seized from the Hill Gmail That Has Not Been Identified as Responsive to the Warrant in Over Two Years Since its Seizure 17

IV. THE GOOD FAITH EXCEPTION DOES NOT APPLY WHERE THE WARRANT WAS SO OVERBROAD THAT AN OFFICER'S RELIANCE UPON IT WAS UNREASONABLE 18

CONCLUSION 19

TABLE OF AUTHORITIES

Page(s)

Cases

In re [REDACTED]@gmail.com,
62 F. Supp. 3d 1100 (N.D. Cal. 2014) 14, 17, 18

Franks v. Delaware,
438 U.S. 154 (1978).....9

Maryland v. Garrison,
480 U.S. 79 (1987).....8

Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,
25 F. Supp. 3d 1 (D.D.C. 2014).....14

United States v. Blake,
868 F.3d 960 (11th Cir. 2017) 14

United States v. Carey,
172 F.3d 1268 (10th Cir. 1999) 14

United States v. Galpin,
720 F.3d 436 (2d Cir. 2013).....8

United States v. Ganias,
824 F.3d 199 (2d Cir. 2016) (en banc).....18

United States v. George,
975 F.2d 72 (2d Cir. 1992).....16, 19

United States v. Leon,
468 U.S. 897 (1984).....18

United States v. Marin Buitrago,
734 F.2d 889 (2d Cir. 1984).....12

United States v. Metter,
860 F. Supp.2d 205 (E.D.N.Y. 2012) 17

United States v. Peraire-Bueno,
No. 24 Cr. 293 (JGLC), 2025 WL 1144745 (S.D.N.Y. Apr. 17, 2025) 9

United States v. Rajaratnam,
719 F.3d 139 (2d Cir. 2013).....9

United States v. Singh,
390 F.3d 168 (2d Cir. 2004).....11

United States v. Ulbricht,
858 F.3d 71 (2d Cir. 2017).....8, 13

United States v. Walser,
275 F.3d 981 (10th Cir. 2001) 14

United States v. Wey,
256 F. Supp. 3d 355 (S.D.N.Y. 2017).....17, 18, 19

United States v. Zemlyansky,
945 F. Supp. 2d 438 (S.D.N.Y. 2013).....16

Wyoming v. Houghton,
526 U.S. 295 (1999).....8

Zurcher v. Stanford Daily,
436 U.S. 547 (1978).....11

Statutes

18 U.S.C. § 1960.....4

18 U.S.C. § 2703.....3

31 U.S.C. § 5330.....4

Other Authorities

31 C.F.R. § 1010.100(ff).....5

31 C.F.R. § 1022.210(a).....5

Fed. R. Crim. P. 41(g).....17, 18

U.S. Const. amend. IV ..... *passim*

Defendant William Lonergan Hill respectfully moves to suppress all evidence that the Government obtained through an unlawful seizure and search of his personal email account, [redacted] ("Hill Gmail"), and for an Order requiring the Government to return or destroy the seized electronic data that has not been identified as responsive to the warrant after over two years.

PRELIMINARY STATEMENT

By March 2023, the Government had been investigating "Samourai Wallet"—a cryptocurrency business suspected of operating as an unlicensed money transmitter and facilitating money laundering by users of its app—for six months. In addition to the publicly available information on Samourai's website and social media accounts, the Government had already sought and obtained warrants to seize all data from the key business email accounts used to conduct Samourai's business. These records identified Mr. Hill, by name and photograph, as Samourai's Chief Technology Officer, as well as the other individuals responsible for Samourai's operations. And they included tens of thousands of documents—including email correspondence, financial statements and spreadsheets, investor and marketing presentations, contracts with vendors, and other business records—detailing "the who, what, when, where, why and how" of the allegedly criminal conduct.

Notwithstanding the previous seizure of these voluminous business records, the affidavit in support of the Government's March 7, 2023, application for a warrant to search Mr. Hill's personal Gmail account stated, falsely, that "[l]aw enforcement officers have not yet identified the individuals who control Samourai's day-to-day operations." Mazur Decl. Ex. 1 (Aff. Special Agent Yohanna Peña ("Peña Affidavit") ¶ 9(e)). The affidavit also omitted any description of the tens of thousands of records it had already seized, misleadingly stating that 90 emails between Samourai accounts and Mr. Hill's personal email account and the metadata of an unspecified

number of emails somehow indicated that the personal account was being "actively used to operate and further Samourai's business." *Id.* These materially false and misleading allegations formed the basis for the seizure and search of a vast trove of Mr. Hill's personal data—including emails, photographs, web searches, personal purchases, finances, and travel history. The Court should therefore suppress the fruits of this unlawful seizure and search or, at a minimum, order a *Franks* hearing.

In any event, the warrant application—with or without the false and misleading statements—failed to establish probable cause to believe that evidence of any crime would be found in Mr. Hill's personal Gmail account. To begin with, based on the law as set forth in the warrant application, there was no probable cause to believe that Samourai was an unlicensed money transmitting business required to obtain a money transmitting license and implement an anti-money laundering program. Moreover, even assuming that Samourai's users were engaged in money laundering or other crimes—with or without the express or tacit consent of its operators—there was no probable cause to believe that Mr. Hill's personal email account would contain evidence relating to those users. If the Government could establish probable cause in this way, then it would have carte blanche to search the private emails of virtually any person suspected of committing crimes at work.

Finally, the search warrant for Mr. Hill's personal email account imposed no meaningful limits on what the Government was allowed to search, authorizing agents to search every record seized for virtually anything that could show who Mr. Hill communicated with and what he was doing. No reasonable law enforcement officer could rely on such a broad general warrant in good faith, particularly where the Government actively misled the Magistrate by falsely stating in the

warrant application that it had not yet identified the individuals controlling Samourai's operations and that Mr. Hill might be managing the business from his personal account.

All evidence seized from the Hill Gmail, as well as any additional evidence obtained as a result of the unlawful seizure and search, must therefore be suppressed pursuant to the Fourth Amendment. In addition, the Court should order the Government to return or destroy any data seized from the Hill Gmail that has not been identified as responsive to the search warrant in over two years.

BACKGROUND

On March 7, 2023, the Government sought and obtained a warrant under 18 U.S.C. § 2703 to seize and search the Hill Gmail.[1] Mazur Decl. Ex. 2. The warrant application was supported by the sworn affidavit of Special Agent Yohanna Peña of the Federal Bureau of Investigation. *Id.* Ex. 1. According to the Peña Affidavit, since about August 2022, the Government had been conducting an investigation of a cryptocurrency business known as "Samourai," which "offere[d] multiple services to its customers that may be used by criminals to launder the proceeds of their criminal activities on the Internet." *Id.* (Peña Aff. ¶ 8). The affidavit further stated that "law enforcement agents currently are seeking to confirm whether [Mr. Hill and his co-defendant, Keonne Rodriguez were] controlling Samourai, and to identify any other individuals who are responsible for Samourai's day-to-day operations." *Id.* (Peña Aff. ¶ 9(e)).

Before it sought to seize the entire contents of Mr. Hill's personal email account, however, the Government already knew the information it purported to be seeking. It had already sought and obtained the entire contents of Samourai's primary business email accounts, including

[1] The warrant also authorized the seizure and search of two other Gmail accounts ([redacted] and support@samouraiwallet.com), but this motion concerns only the Hill Gmail.

wallet@samourai.com and dev@samourai.com. These Samourai accounts, comprising tens of thousands of documents, contained extensive information about Samourai's operations, including Mr. Hill's role as Chief Technology Officer. The records already seized by the Government included, for example, an investor presentation in which Mr. Hill was identified by name, next to his photograph, and a short biography. *See* Mazur Decl. Ex. 3 at 5.

The records also included records of how Samourai was conducting its business, which showed that it was being managed through the Samourai business email accounts. By way of example only, they included:

- business plans, which again included Mr. Hill's name and photograph, along with other Samourai personnel, *id.* Ex. 4;
- reports to Samourai's investors, *id.* Ex. 5;
- service provider agreements identifying Mr. Hill as the person from whom the provider would take direction, *id.* Ex. 6;
- financial data, *id.* Ex. 7, 8;
- board materials, *id.* Ex. 9; and
- myriad business correspondence, *id.* Exs. 10, 11, 12, 13, 14, 15.

Special Agent Pena's Statements Purporting to Establish Probable Cause

In her affidavit seeking a warrant for the Hill Gmail, Special Agent Peña sought to demonstrate probable cause that (1) Samourai was operating as an unlicensed money transmitting business that facilitated money laundering, Mazur Decl. Ex 1 (Peña Aff. ¶¶ 10-22); and (2) the Hill Gmail was "actively used to further Samourai's business," *id.* (Peña Aff. ¶¶ 22(b)-(c) & 25).

First, the Peña Affidavit attempted to establish probable cause that Samourai was an "unlicensed money transmitting business" under 18 U.S.C. § 1960. It therefore described the

requirements for registration of "money transmitting businesses" under the Bank Secrecy Act ("BSA"). *Id.* (Peña Aff. ¶ 10 (citing 31 U.S.C. § 5330)). As explained in the affidavit, the Secretary of the Treasury had "the authority to establish which individuals and entities are subject to the registration requirement contained in 31 U.S.C. § 5330." *Id.* (Peña Aff. ¶ 10(c)). Those regulations, in turn, required registration of any "money services business," including a "money transmitter"—defined as a business engaged in "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." *Id.* (citing 31 C.F.R. § 1010.100(ff)). The BSA further requires that such businesses "maintain an 'effective anti-money laundering compliance program … reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities.'" *Id.* (Peña Aff. ¶ 10(d) (citing 31 C.F.R. § 1022.210(a))).

The affidavit also described certain "regulatory guidance" issued in 2019 by the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") "making clear that cryptocurrency mixers or tumblers that provide 'anonymizing services'—*i.e.*, services that 'accept [cryptocurrency] and retransmit [it] in a manner designed to prevent others from tracing the transmission back to its source'—are subject to the BSA." *Id.* (Peña Aff. ¶ 10(e)). But, "[i]n contrast, 'anonymizing software providers'—*i.e.*, suppliers of software a transmitter would use for the same purpose' (emphasis in original), are not subject to the BSA." *Id.* Such software providers are not considered money transmitters and "[are] not subject to the BSA … because, like any other 'supplier[] of tools (communications, hardware, or software) that may be utilized in money transmission,' [they are] engaged in trade and not money transmission." *Id.*

Special Agent Peña stated that she had learned from other law enforcement agents that "at no point has Samourai been registered with FinCEN," the "component of the Treasury that keeps records of money transmitting business who are registered with the Treasury Department[.]" *Id.* (Peña Aff. ¶ 12). Nor could she identify any "know your customer" or "KYC" requirements for users of Samourai or "any other AML or sanctions compliance controls that Samourai ha[d] implemented." *Id.* (Peña Aff. ¶ 13).

The Peña Affidavit then set forth—at length—various public "Tweets" and "Public Telegram Messages," from which it concluded that Samourai was intended to be used as a means for users to launder illicit funds. *Id.* (Peña Aff. ¶¶ 16-21). And it cited a "PowerPoint slide deck from 2015," obtained through prior seizures of Samourai data, referring to "Dark/Grey Market Participants" and "Online Gamblers" as potential Samourai customers. *Id.* (Peña Aff. ¶ 22(a)).

Second, in an attempt to show probable cause that Mr. Hill's personal Gmail account would contain relevant evidence, Special Agent Peña described her review of records received from an earlier § 2703(d) order directed at Google. The affidavit states that, "between August 6, 2015, and January 14, 2019," the Hill Gmail had "approximately 90 emails in its mailbox to or from Samourai-related e-mail accounts," including dev@samouraiwallet.com, samouraidev@tuta.io, wg@samourai.io, tdevd@samourai.is, and [redacted]. *Id.* (Peña Aff. ¶ 23(b)). The affidavit further states that, "between September 13, 2015, and December 19, 2018, [the Hill Gmail] sent emails to or received emails from … [six specified] digital currency and business support email accounts[.]" *Id.* Finally, Special Agent Peña stated that, "[b]ased on my review of files and attachments to emails sent to or from Subject Account-1 and [the Hill Gmail], the 'subject' lines of these emails, and the senders and recipients of these emails," an unspecified number of the emails appeared to relate to Samourai's business. *Id.* (Peña Aff. ¶ 23(c)).

Scope of Evidence Sought

Based on these sworn statements from Special Agent Peña, the Government sought and received authorization to seize and search a vast trove of Mr. Hill's personal data. The Warrant ordered Google to produce, for a period from January 1, 2015 to March 2023, "all emails sent to or from, stored in draft form in, or otherwise associated with" the Hill Gmail, data from dozens of Google services (including Google Calendar, Google Drive, Location History, YouTube, Google Photos, and Google Play Music), subscriber and payment information, Chrome browser and web search history records, device information, information regarding linked accounts, transactional records, and customer correspondence. Mazur Decl. Ex. 2 (Warrant Attachment at 1-5). The warrant further authorized the Government to search through all of this data, without any restrictions, in order to identify any evidence of operating an unlicensed money transmitting business, money laundering, or sanctions violations. *Id.* at 3-5.

Data Seized from the Hill Gmail

In response to the warrant, Google produced 154,013 files to the Government from the Hill Gmail account. These files included vast quantities of Mr. Hill's personal data completely unrelated to Samourai that the Government was allowed to search indiscriminately. The data included Mr. Hill's personal email correspondence, records of personal purchases, photographs, and his Google calendar detailing personal engagements and travel.

To date, the Government has identified only five documents from the Hill Gmail as actually responsive to the warrant: three records of Mr. Hill's personal Google search history and the device information associated with Mr. Hill's account. Mazur Decl. Exs. 16, 17, 18, 19, 20.

LEGAL STANDARD

Under the Fourth Amendment, "the right of the people to be secured in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and

no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Searches of a person's digital data pose a special threat to privacy because of the high volume and wide variety of personal data often held on a person's internet accounts, or digital devices. *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017) ("A general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be 'akin to a residence in terms of the scope and quantity of private information [they] may contain") (internal citation omitted); *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (this privacy "threat demands a heightened sensitivity to the particularity requirement in the context of digital searches").

Even where the Government establishes probable cause to seize and search personal data, the particularity requirement holds that the scope of any search must correspond to that of the probable cause underlying the warrant. "By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [Fourth Amendment] ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see also Wyoming v. Houghton*, 526 U.S. 295, 300 (1999) (the reasonableness of a search may be determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate Governmental interests").

ARGUMENT

I. THE PEÑA AFFIDAVIT CONTAINED FALSE AND MISLEADING STATEMENTS THAT ARE MATERIAL TO PROBABLE CAUSE

A defendant is entitled to a *Franks* hearing where he makes a "substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth was included by the affiant in the warrant affidavit, and if the allegedly false statement [was] necessary to the finding of probable cause." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). Once "a defendant makes a preliminary showing that the Government's affidavit misstated or omitted material information, *Franks* instructs a district court to hold a hearing to determine whether the alleged misstatements or omissions in the warrant or wiretap application were made intentionally or with reckless disregard for the truth and, if so, whether any such misstatements or omissions were material." *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013); *see also United States v. Peraire-Bueno*, 2025 WL 1144745 at *2 (S.D.N.Y. Apr. 17, 2025) (granting Defendant's motion for a *Franks* hearing where "statements that Defendants contend[ed] [were] false appear[ed] to be directly in conflict with publicly-available information and information cited in the affidavits themselves.").

When the Government sought the Hill Gmail warrant, it already knew that Mr. Hill was one of the founders and operators of Samourai Wallet. The documents the Government had already seized from the Samourai emails included PowerPoint slide decks for potential investors, business plans, and contractual agreements that identified Mr. Hill by name and photograph as a Co-Founder and Chief Technology Officer. Mazur Decl. Ex. 3 at 5; Ex. 4 at 42; Ex. 6 at 1. Also in the Government's possession prior to applying for the Gmail warrant was Google Subscriber information listing Mr. Hill's full name and both UK and French telephone numbers, which the

Government obtained through the earlier § 2703(d) order for records relating to his personal account. Mazur Decl. Ex. 21.

It was therefore highly false and misleading to suggest that the Government had "not yet identified the individuals who control Samourai's day-to-day operations." *Id.* Ex. 1 (Peña Aff. ¶ 9(e)). Having previously confirmed Mr. Hill's identity, as well as that of his co-defendant and others involved in the business, the Government was simply seeking to conduct an unfettered search through Mr. Hill's personal email and other data in the hope that it would uncover incriminating evidence, whether related to Samourai or not.

Special Agent Peña's affidavit not only misled the court as to the reason for the search of Mr. Hill's private records, but also misleadingly failed to describe the records it had already obtained, which showed that Samourai's *business* accounts were being used to actively manage the business. The documents previously seized included all manner of business correspondence, financial records, contracts, presentations, and other records relating to Samourai's business. *See* Mazur Decl. Exs. 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15.

In context, the fact that there were 90 emails to or from Mr. Hill's personal account over a period of more than three years—fewer than three emails a month—did not remotely show that it was being used to "actively manage" the business, as the Peña Affidavit asserted. Nor do interactions between a personal email account and cryptocurrency services not affiliated with Samourai suggest that those communications had anything to do with Samourai, much less that they would contain evidence of criminal activity. Indeed, the Government knew at the time that the volume of files seized from the Samourai emails was more than 900 times greater than the 90 emails the Government identified as connected to Mr. Hill's personal Gmail. On this basis, the

Court should suppress the data obtained pursuant to the Gmail warrant or, at a minimum, order a *Franks* hearing.

II. THERE WAS NO PROBABLE CAUSE TO CONCLUDE THAT SAMOURAI WALLET WAS AN UNLICENSED MONEY TRANSMITTING BUSINESS OR THAT EVIDENCE OF MONEY LAUNDERING OR OTHER CRIMES BY ITS USERS WOULD BE FOUND IN MR. HILL'S PERSONAL GMAIL ACCOUNT

The probable cause requirement of the Fourth Amendment demands "a sufficient nexus between the criminal activities alleged" and the location or items searched. *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004); *Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978) ("The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought."). Such a nexus "may be based on reasonable inference from the facts presented based on common sense and experience." *Singh*, 390 F.3d at 182 (internal citations omitted).

A. The Peña Affidavit Failed To Establish Probable Cause To Conclude That Samourai Wallet Was An Unlicensed Money Transmitting Business

The Peña Affidavit failed to establish probable cause to conclude that Mr. Hill's Gmail would contain evidence that Samourai was an unlicensed money transmitting business because, under the very rules and regulations described in the affidavit itself, Samourai was in fact, not such a business. As the affidavit states, Samourai was a non-custodial wallet, never accepting nor transmitting any cryptocurrency, because its users conducted their own transactions without surrendering control of their cryptocurrency by sharing their "private keys." Mazur Decl. Ex. 1 (Peña Aff. ¶ 9(a)). Samourai was therefore not a money transmitter, meaning that it was not required to register with FinCEN or implement anti-money laundering controls.

Because Samourai Wallet was not a money transmitter, there was no basis to conclude that Mr. Hill was operating an unlicensed money transmission business. Indeed, this is clear from the

FinCEN guidance cited in the affidavit itself. *Id.* Ex. 1 (Peña Aff. ¶ 10(e)) ("[A]n anonymizing software provider is not subject to the [Bank Secrecy Act] because, like any other 'supplier of tools (communications, hardware, or software) that may be utilized in money transmission' it is 'engaged in trade and not money transmission.'"). That Samourai would not require a license with FinCEN was confirmed to the Government no later than August 23, 2023, when FinCEN's Chief of Virtual Assets and Emergency Technology Section in the Enforcement and Compliance Division told the prosecutors in this case that FinCEN's guidance had focused on the question of "custody," such that Samourai would not have qualified as a money transmitter.[2] That Mr. Hill's personal email account had 90 communications with Samourai accounts and contained an unspecified number of other emails that appeared to relate to Samourai provided no probable cause to believe that the personal email would contain evidence relating to the operation of an unlicensed money transmission business because Samourai was not engaged in money transmission at all.

B. The Peña Affidavit Failed To Establish Probable Cause That Evidence of Money Laundering or Sanctions Evasion Would Be Found in Mr. Hill's Personal Gmail Account

Nor did Special Agent Peña's characterization of her review of the returns of the § 2703(d) order on Mr. Hill's Gmail establish probable cause to believe that there would be any evidence of money laundering or sanctions evasion in Mr. Hill's Gmail account. Indeed, the Peña Affidavit provides no explanation of how these documents would constitute evidence of unlicensed money transmitting, money laundering, or any other crime. Evidence that Samourai's *users* may have

[2] *See* ECF No. 86. Even if the Government disagreed with FinCEN's interpretation of the law and its own guidance, once the Government learned FinCEN's position with respect to Samourai Wallet, it should have updated the Magistrate and corrected its prior representations in light of the changed circumstances. *United States v. Marin Buitrago*, 734 F.2d 889, 894 (2d Cir. 1984) ("[W]hen a definite and material change *has* occurred in the facts underlying the magistrate's determination of probable cause, it is the magistrate, not the executing officers who must determine whether probable cause still exists. Therefore, the magistrate must be made aware of any material new or correcting information.").

been laundering money provides no basis to believe there would be evidence of those crimes in Mr. Hill's personal Gmail account.

The pittance of responsive materials the Government has identified to date when compared to the much larger number of Samourai-related documents in the actual Samourai business accounts only confirms the absence of probable cause to search the personal account. Nothing in the Peña Affidavit established probable cause that a search of the Hill Gmail would yield evidence of any crime. It was instead a fishing expedition to see if trolling through Mr. Hill's personal data might yield something incriminating. The evidence obtained through the seizure and search of the personal account should be suppressed.

III. THE GMAIL SEARCH WARRANT WAS IMPERMISSIBLY OVERBROAD UNDER THE FOURTH AMENDMENT

A. Where the Underlying Probable Cause is Narrow, Search Warrants Authorizing the Wholesale Search and Seizure of a Person's Email Account are Impermissible Under the Fourth Amendment

With the proliferation of personal information contained in electronic form, courts have expressed growing concern that search warrants enabling the wholesale search of a defendant's email, computer files, or social media accounts, where the underlying probable cause is narrow in scope, may violate the Fourth Amendment's protections. In extraordinary cases, it may be permissible to seize and search an entire laptop computer or personal email account where the Government demonstrates that a subject used the computer or account to operate an unlawful enterprise. *See Ulbricht*, 858 F.3d at 102 ("Ulbricht used his laptop to commit the charged offenses by creating and continuing to operate Silk Road. Thus, a broad warrant allowing the Government to search his laptop for potentially extensive evidence of those crimes does not offend the Fourth Amendment[.]").

But in most cases the special dangers posed by seizures of electronic data require the Government to implement narrowing mechanisms in its search methods to bring search warrants for electronic data in accord with the Fourth Amendment. Such mechanisms include key word searches, date restrictions, or requiring the Government to destroy non-responsive data. *See United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. 1999) (reversing the District Court's denial of defendant's suppression motion, finding the Government exceeded the scope of its warrant by failing to employ mechanisms to limit its search to data responsive to the warrant); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (denying a warrant application that would grant the wholesale seizure and search of a defendant's Gmail, stating the Government's request was not "reasonable in the Fourth Amendment sense of the word" where the Government did not at least provide a date restriction); *Matter of the Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 25 F. Supp. 3d 1 at *8 (D.D.C. 2014) (denying an email search warrant that did not employ "minimization procedures" because the Court was "unwilling to issue any search and seizure warrants for electronic data that ignore the constitutional obligations to avoid 'general' electronic warrants"); *see also United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) ("[o]fficers must be clear as to what they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant"); *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017) (procedures limiting disclosures to communications involving other members of the conspiracy, or data from the relevant time period "would have undermined any claim that the Facebook warrants were the internet version of a 'general warrant'").

The Government should have been required to employ such limiting mechanisms in its search of Mr. Hill's personal Gmail account to prevent the execution of an impermissible general

warrant. The Peña Affidavit identified several Samourai-related email accounts Mr. Hill's Gmail had interacted with. Mazur Decl. Ex. 1 (Peña Aff. ¶ 23(b)). It also identified categories of Samourai-related documents the Warrant was targeting, including "Samourai business plans" and "Samourai independent contractor agreements." *Id.* (Peña Aff. ¶ 23(c)). The level of specificity with which the Government was able to identify the kinds of "responsive" data likely to be found in the account indicates that it could have employed targeted search tactics rather than inspecting every single file. Had the Government used a more targeted approach, the Gmail warrant might have been saved from defective overbreadth.

B. The Warrant Did Not Provide Meaningful Guidance As To What Data Fell Within The Purview Of The Warrant

What limiting mechanism the Warrant did impose—a list of categories of data "responsive" to the warrant—was itself so expansive that it provided no meaningful Fourth Amendment protection. Indeed, the very first category of data the Government labels "responsive" to the Warrant is so broad as to swallow any purported limitations:

> "Information identifying the user(s) of the Subject Accounts and the individuals involved in the Subject Offenses as well as their location(s), including photographs or videos depicting the user(s) of the Subject Accounts and communications with individuals that the user(s) of the Subject Accounts trust, which reveal their identities, such as travel information, receipts for online purchases, communications with social network websites or third party service providers, or the devices they used;" Mazur Decl. Ex. 2 (Warrant Attachment at 4).

The Government was thus authorized to search in-depth, material of the utmost intimate and personal nature of their suspects—communications with people they "trust," online purchases, use of "social network sites," photographs, and travel history, all from a personal account—whether it related to Samourai or not. The Government's diverse list of exemplary data illustrates the key issue: just about anything could qualify as identifying information. And, therefore, the entirety of

the account could be "responsive" to the warrant, depending on the discretion of the executing officer.

The Warrant further authorized the seizure of "[e]vidence that may reveal the identities of and/or relationships between Samourai's creators, operators, management, and associates." *Id.* This leaves the executing officer with no guidance as to what evidence may or may not be helpful to determine the identities of "associates" of Samourai Wallet, or how they should search for information revealing the relationships between unidentified individuals. The provision permitting the seizure of "[e]vidence that may identify assets, including bank accounts and digital or virtual currency accounts, that may represent proceeds of the Subject Offenses" is similarly amorphous, and all-encompassing. *Id.* Again, the executing officer is free to conclude that everything may be helpful, and therefore "responsive." The combined effect of the categories purporting to narrow the search's scope in actuality encompasses the entirety of the Hill Gmail.

Courts in the Second Circuit have found warrants invalid where they were so broad as to fail to provide necessary guidance as to what data is "responsive" to the warrant. *See United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992) ("The instant warrant's broad authorization to search for any other evidence relating to the commission of a crime plainly is not sufficiently particular with respect to the things to be seized because it effectively granted the executing officers virtually unfettered discretion to seize anything they [saw]") (citations and quotation marks omitted). Warrants with such broad instructions, "suffer from ambiguity" and "could afford a reasonable officer extremely broad discretion in deciding what items" fall within their scope. *See United States v. Zemlyansky*, 945 F. Supp. 2d 438, 459 (S.D.N.Y. 2013). These considerations are even more crucial when "responsive" evidence is intermingled with "non-responsive" evidence, as is frequently the case with electronic files, and even more so in this case, where the Government

searched Mr. Hill's entire personal email based on a small number of emails that may have related to Samourai. *See United States v. Wey*, 256 F. Supp. 3d 355, 386 (S.D.N.Y. 2017) ("[A] more particular description than otherwise might be necessary is required when other objects of the same general classification are likely to be found at the particular place to be searched") (citations and quotation marks omitted). The evidence obtained pursuant to the overreaching Gmail Warrant must be suppressed.

C. The Government Must Return or Destroy Any Data Seized from the Hill Gmail That Has Not Been Identified as Responsive to the Warrant in Over Two Years Since its Seizure

The Government sought and obtained permission to seize and search the Hill Gmail over two years ago. Since then, it has had unfettered access to a trove of Mr. Hill's personal data and has identified only five documents as responsive to the Warrant. The data that has not been identified as responsive—consisting of all manner of personal information, including correspondence, photographs, financial information, purchase histories, web searches, and location information—comprises some of the most intimate, personal records imaginable.

Rule 41(g) of the Federal Rules of Criminal Procedure authorizes "[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property" to move for its return. Whether or not the Court holds that the seizure and search of the Hill Gmail was unlawful, Mr. Hill remains aggrieved by the continued seizure of the voluminous personal data for over two years. Indeed, the Government's retention of the data constitutes an ongoing violation of the Fourth Amendment. *See United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012) ("[T]he Fourth Amendment requires the Government to complete its review, i.e., execute the warrant, within a "reasonable" period of time."); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d at 1104 (concluding, in part based on the absence of "any commitment to return or destroy evidence that is not relevant to its investigation," that the "unrestricted right to retain and use every

bit Google coughs up undermines the entire effort the application otherwise makes to limit the obvious impact under the plain view doctrine of providing such unfettered Government access").

Having had ample time to review the Hill Gmail for information responsive to the Warrant, and there being no indication that the unidentified data is responsive, the Government should be ordered to return or destroy it. *See United States v. Ganias*, 824 F.3d 199, 219 (2d Cir. 2016) (en banc) ("Rule 41(g) thus provides a potential mechanism, in at least some contexts, for dealing with the question of retention at a time when the Government may be expected to have greater information about the data it seeks and the best process through which to search and present that data in court."); *see also id.* at 226 (Lohier, C.J., concurring) (approving the use of Rule 41(g) "when faced with the Government's retention of electronic data").

IV. THE GOOD FAITH EXCEPTION DOES NOT APPLY WHERE THE WARRANT WAS SO OVERBROAD THAT AN OFFICER'S RELIANCE UPON IT WAS UNREASONABLE

The Government may not avail itself of the "good faith" exception to the rule that evidence obtained pursuant to a defective warrant must be suppressed. For the good faith exception to apply, the executing officer's reliance on the warrant "must be objectively reasonable." *United States v. Leon*, 468 U.S. 897, 922 (1984). But "a warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id.* at 23; *see also Wey*, 256 F. Supp. 3d at 399 (S.D.N.Y. 2017) ("[E]xecuting officers could not reasonably rely on warrants that were so lacking in particularity as to be 'general in nature'") (internal citation omitted).

The breadth of what the Government sought to seize here—including any information about who Mr. Hill communicated, who he "trusted," what he searched for on the internet, his finances, what he purchased, and where he went—dramatically illustrates the problem. *Cf. Wey*, 256 F. Supp. 3d at 398 (granting suppression where warrants "authorize[d] the seizure of multiple

expansive categories of records (e.g., 'notes,' 'memoranda,' 'correspondence," 'communications,' 'photographs,' etc.) without any meaningful linkage to the suspected criminal conduct and limited only, at the outer boundaries, to some relationship to the owner/occupant of the premises being searched"). It was simply not reasonable for the Government to obtain and review the entire contents of Mr. Hill's personal Gmail account spanning almost a decade based on the existence of a handful of Samourai-related documents in the account and what amounted to no more than the Government's hope that the personal account would contain incriminating evidence. Here, moreover, the absence of good faith is even more obvious, where the Government already knew the information it claimed to be searching for in the Hill Gmail based on its prior search of the Samourai business accounts, including the identities of Mr. Hill and the others who were operating the business. In these circumstances, the Government cannot meet its burden "to demonstrate the objective reasonableness of the officers' good faith reliance" on the defective warrant, and the evidence should therefore be suppressed. *George*, 975 F.2d at 77.

CONCLUSION

For the foregoing reasons, the Court should suppress the entirety of the evidence seized from the Hill Gmail account, as well as any additional evidence obtained as a result of the Government's search of the Hill Gmail account, and order the Government to return or destroy all personal data seized from the Hill Gmail account that has not been identified as responsive to the Warrant.

Dated: May 29, 2025

Respectfully submitted,

By: *Roger A. Burlingame*

Roger A. Burlingame
Matthew L. Mazur
DECHERT LLP
Three Bryant Park
1095 Avenue of the Americas

New York, NY 10036
Tel.: +1 212 698 3500
roger.burlingame@dechert.com
matthew.mazur@dechert.com

Counsel for Defendant William Lonergan Hill